NATIONAL DEFENSE UNIVERSITY
STRATEGIC FORUM
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Number 35, July 1995

The Next Enemy

Author: Martin C. Libicki, Senior Fellow

Note:

Conclusions

Recommendations

About the Workshop

Discussion

The Cold War offered military planners considerable strategic clarity the threat was known, and the problem was generating a force structure of sufficient size and sophistication to counter it. Today's military threats are varied and, for the most part, well below the level that even a shrinking U.S. force can handle comfortably. Threats ten to twenty years out, however, must be taken seriously because of the long time required to complete a major systems acquisition; to develop, test, and institutionalize new doctrine; and to accomplish the organizational innovations necessary to use both effectively.

Future threats may be divided into four categories: peers, bullies, terrorism, and chaos. The threat environment twenty years hence is unlikely to be of one type. Nevertheless, framing the choices facing planners shows what the U.S. armed forces might look like if one or another type of threat were to become the predominant focus of the Defense Department.

Peers

Few planners think it likely that the next twenty years will see a reemergence of a nation that can pose a challenge to U.S. military power as broadly as the Soviet Union did. However, at least two countries (Russia and China) could conceivably be peer adversaries at the strategic level of nuclear weapons, space, and information systems. Others could come close. How should the United States respond to the possibility? One avenue of interaction is to use arms controls to manage the cost of competition and the consequences of interstate breakdown. New restrictions on land warfare (e.g., tagging heavy equipment, placing sensors in border areas, putting size limitations on ground forces) would benefit the United States, given its compact army. On the other hand, some participants agreed that some of today's arms control regimes should be rolled back. Many felt that the United States is overly restricted in space and that a more permissive ABM regime would serve U.S. interests. Yet if the world's superpower stepped away from mutual arms limitations, this might send the wrong message about U.S. intentions and complicate counter-proliferation efforts.

Another avenue of future competition may be information warfare. Can or should the United States hold other nations' participation in the world economy at risk? The United States might be able to shut down another nation's banking system but not without risk of collateral damage to the global banking system. Can physical war be replaced by a survival contest among rival information systems under attack? Perhaps the United States should concentrate on developing defensive systems. The United States has the biggest stones, but also the most glass in its house.

What can the United States do to deter peer-level competition? Perceptions management was held to be key to U.S. national security. Most believed that the stronger and more capable the United States showed itself to be, the less often it would be challenged by others. Yet, with coalitions unstable, a demonstration of U.S. power might persuade others to ally themselves against what they would perceive as their leading threat (e.g., German behavior between 1890 and 1914).

A world of peer strategic competition would drive the military in familiar directions towards: nuclear forces, satellites and other long-range warning systems; tactical ballistic missile defense systems (including for allies); perhaps strategic defense systems and space attack systems; air defense in general; information warfare and security; and robust command-and-control.

Bullies

If the circumstances and logic of the Bottom Up Review hold true for two more decades, U.S. armed forces will be sized and structured primarily to engage in two simultaneous major regional contingencies (MRCs). The usual suspects in such MRCs (e.g., Iran, Iraq, North Korea) are presently unsophisticated rogue states that aspire to nuclear weapons and delivery systems. Conference participants believe that U.S. forces could cope with the challenges of future conventional warfare, even if force levels continue to diminish. However, two events would make the United States rethink its strategy nuclear weapons proliferation, and the sophisticated exploitation of world technology markets.

The presence of nuclear weapons is likely to alter the U.S. approach to MRCs. Cold War deterrence was stable because both sides understood the rules of the game rules that new nuclear states may not accept. Should the United States say what circumstances warrant a nuclear response or leave distinctions fuzzy? Many war game participants hesitate to retaliate in kind following a nuclear strike even against U.S. forces. It is less likely that the United States would retaliate against chemical or biological weapons by nuclear means. If the United States forgoes retaliation by weapons of mass destruction (WMD), would U.S. conventional warfighting capabilities provide sufficient deterrence?

Geography suggests that many threats from WMDs will be directed against U.S. allies before they are directed against the United States (e.g., by radical Islamic states against southern Europe, by North Korea against a wavering Japan). The United States has a range of systems it could offer allies. Yet, with future alliances inherently uncertain, careful judgements must be made about how much ballistic and theater missile defense technology the United States can prudently transfer.

Alternatively, an MRC opponent may be able to avoid going to the nuclear threshold by a strategy which uses smart munitions, commercial command-and-control, and a variety of surveillance technologies (e.g., unmanned aerial vehicles, third-party satellite surveillance) to exact damaging casualties on U.S. forces. The United States has two major asymmetries to consider in conflicts that do not affect its national security directly. One is a longer logistics chain; the other is sensitivity to casualties.

The American public has grown increasingly reluctant to shed American blood (or even enemy blood as the CNN-fed reaction to Iraqi casualties suggests). In a violent world, how might that limit the U.S. military; might it be judged solely by casualties? So-called non-lethal technologies offer scant relief since many can kill. Even information warfare can kill if it disables critical societal systems. History suggests that warfare is inevitably violent and ugly, and the lethality of weapons will continue to rise.

Many war games analyze whether new technology will let the United States refight the Gulf War more efficiently; few refight the Vietnam War to see if technology makes the United States more effective under those circumstances.

If the U.S. armed forces were shaped to conduct MRCs alone, it would initially look much like today's with an emphasis on heavy maneuver forces, combat naval groups, and air power. Against a foe with nuclear or other weapons of mass destruction, the United States would have to think about operational innovations that minimize and disperse its logistics, command, and combat infrastructures; some of them would have to work from long stand-off ranges. Against a sophisticated regional foe, the United States might not want to use platforms at all but rely on a combination of stand-off attack forces, and information-based warfare assets (for giving targeting data to local coalition partners), coupled with special operations forces used for liaison and other tasks.

Terrorism

Largely because of the limited capability that classical military instruments have in coping with terrorism, conference participants kept returning to the threat that it may pose to U.S. national security. Incidents may range from the use of conventional explosives (e.g., what if the van in the World Trade Center explosion had been parked in a more vulnerable spot), to nuclear or chemical weapons, biological agents, and their analogue in cyberspace information warfare.

Devices that can cause terror are getting easier to manufacture and transport and harder to detect. The equipment for replicating biological agents is inexpensive; the equipment for replicating computer agents is even cheaper. Many otherwise third-world Asian nations have very large computer-literate cohorts that make them potential information warfare powers.

Understanding terrorism as an act of war is complicated by two connections: between the act and the individual or group that commits the act, and between the perpetrators and a state or proto-state (e.g., guerilla groups). Even when organizations come forward to claim responsibility, it is not always easy to convict individuals on the basis of judicial-quality evidence. Perpetrators may or may not be supported by foreign governments, but the focus is on the actors not the sponsors. Retaliation by the United States against sponsor governments is problematic; thus, so is deterrence.

The lack of links between terrorism and a state also work in reverse. A nation or even an organization cannot easily use terrorism to coerce others if it cannot show it can cause specific acts to happen or prevent them from happening.

What would the U.S. military look like if the primary threat to U.S. national security were terrorism? Crime prevention and prosecution is not considered a military role although some functions may be usefully assigned for special forces. Maintenance of domestic order (e.g., in the aftermath of an attack) would be a higher priority and the United States might even have forces that could be lent to allies for similar missions. In some cases (e.g., state-sponsored information warfare) the United States might want a cohort that can retaliate in kind. There should also be robust ability to retaliate with conventional

measures (e.g., the 1986 air strike into Libya).

Chaos

Over the next two decades, states will continue to fail. Some failures may create circumstances (e.g., refugees, malcontents, and environmental damage) which topple other states. To cope, the United States may need a robust capability to conduct peace and relief operations.

What will DOD's role be in peace operations? The U.S. military has become the jack-of-all-trades for peace operations an overextended role according to some conference participants. Several would have U.S. forces collaborate more closely with civilian agencies. Others would improve interoperability with NGOs (non-governmental organizations) letting the latter do more of the humanitarian work that the military does now. Duties associated with sanctions could be given to non-military units. Alternatively, specific units (e.g., from the Special Operations Command) could be tasked with peace operations. The rest of the military, freed from this mission, would refocus on deterring and conducting warfare.

A concentration on peace operations may also be a good reason to expand foreign military interactions. Improving interoperability with future coalition partners carries many advantages. Yet, above a certain technological level of integration, the risk of exposing information on U.S. capabilities to what may be temporary allies has to be carefully managed.

If countering chaos were the primary mission of the U.S. armed forces, then they would have to become lighter and more mobile (because states often fail with little warning, and the United States usually responds only in extremis). The Army and Marine Corps would have larger roles, while the Navy and Air Force would focus on lift. As emergency operations become the norm, some functions assigned to reserve units may have to be shifted to active ones (e.g., to allow civil affairs assets to be used more frequently).

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: The Next Enemy

B. DATE Report Downloaded From the Internet: 10/03/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **National Defense University Press**
Institute for National Strategic Studies
Washington, DC 20001

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 10/03/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.